REDACTION-FIRST PROTOCOL

Operational Privacy for P-Series Instruments

December 2022

Dr. F. Patterson · Security Working Group

Standard Index Group
1 Lombard Street
London EC3V 9AA
United Kingdom

ABSTRACT

The Redaction-First Protocol establishes privacy-preserving workflows for delegating estate administration tasks to assistants, clerks, or bureau services while maintaining confidentiality of sensitive financial and personal information. Problem Statement: UHNW principals require administrative assistance but face a privacy paradox:

- Administrative tasks require document access
- Full document access exposes sensitive information (account balances, holdings, personal details)
- Assistants don't need full information to perform most tasks
- Traditional "trust-based" access creates unnecessary exposure

Solution: Systematic redaction protocols that preserve task functionality while minimizing information disclosure. Principle: Expose only what is operationally necessary. Redact everything else. Compliance: This protocol implements GDPR Article 5(1)(c) data minimization principles:[1] Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

[1] GDPR (EU) 2016/679 Article 5: Principles relating to processing of personal data.

CORE PRINCIPLES

1. Need-to-Know Basis

Definition: Assistant receives minimum information required to complete assigned task. Example:

- Task: "Update P-02 Accounts Register with new bank branch address"
- Needs: Account name, current address, new address
- Does NOT need: Account number, balance, credentials

Implementation: Redact account numbers and balances before providing document.

---

2. Separation of Duties

Definition: No single assistant has access to complete financial picture. Example Structure:

- Assistant A: Updates P-02 (Accounts) - sees account names, no balances
- Assistant B: Updates P-03 (Assets) - sees holdings types, no valuations
- Assistant C: Updates R-02 (Renewals) - sees expiration dates, no amounts

Advantage: Even if one assistant is compromised, incomplete information limits damage.

---

3. Pointer Preservation

Definition: Assistant must maintain DP references intact even if redacting surrounding content. Example:

```
BEFORE REDACTION:
Account: HSBC Premier (123-456789)
Balance: £2,450,000
Access: See DP-01
AFTER REDACTION:
Account: HSBC Premier ([BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK])
Balance: [BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK]
Access: See DP-01 <- PRESERVED
```

Critical: DP references must remain visible for document usability.

---

4. Annotation Prohibition

Definition: Assistants cannot annotate, comment, or add notes to original documents. Workflow:

- Assistant identifies needed changes
- Documents changes in separate "amendment list"
- Principal reviews amendment list
- Principal makes actual changes to document
- OR: Principal approves, different authorized person implements

Prevents: Accidental exposure via comment metadata or annotation history.

REDACTION TECHNIQUES

Physical Document Redaction:

Method 1: Black Marker (Permanent)

- Use opaque black permanent marker (Sharpie or similar)
- Apply 2-3 overlapping strokes (ensures opacity)
- Test with backlight (hold up to light - no bleed-through)

Method 2: Adhesive Redaction Labels

- Black adhesive labels (non-removable)
- Precisely sized to cover text
- Smooth application (no bubbles/edges)

Method 3: Whiteout + Photocopy

- Apply correction fluid over sensitive text
- Photocopy document (permanent, cannot be reversed)
- Destroy original (if not needed)

Inadequate Methods:

- [NO] Highlighter (text visible underneath)
- [NO] Removable stickers
- [NO] Post-it notes

Digital Document Redaction:

Proper PDF Redaction: Adobe Acrobat Pro:

1. Tools -> Redact -> Mark for Redaction
2. Select sensitive text/areas
3. Apply Redactions (this REMOVES data, doesn't just cover)
4. Save redacted PDF
5. Verify with "Examine Document" tool

Critical: "Apply Redactions" must be clicked - marking alone doesn't remove data.
Inadequate Methods:

- [NO] Drawing black rectangles (text still exists underneath)
- [NO] Highlighting in black (reversible)
- [NO] Text color to white (still selectable)

Verification Test:

- Select all text (Ctrl+A / Cmd+A)
- Copy to text editor
- Redacted content should NOT appear

TASK-SPECIFIC PROTOCOLS

III. TASK-SPECIFIC REDACTION PROTOCOLS

Task: Update Account Addresses

Documents affected: P-02 (Accounts Register) Redact:

- [YES] Account numbers
- [YES] Balances
- [YES] Access credentials (should already be in DP, but verify)

Preserve:

- [NO] Account institution name
- [NO] Current address
- [NO] New address (assistant needs this)
- [NO] DP references

Example redacted entry:

```
+----------------------------------------+
| HSBC Premier |
| Account: [BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK] |
| Address: 123 High Street -> 456 New Road |
| Balance: [BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK][BLOCK] |
| Access: DP-01 |
| Renewal: Annual |
+----------------------------------------+
```

Task: Track Insurance Policy Renewals

Documents affected: P-06 (Policy Index), R-02 (Renewal Registry) Redact:

- [YES] Policy numbers
- [YES] Coverage amounts
- [YES] Premiums

Preserve:

- [NO] Insurer name
- [NO] Policy type (life, property, liability)
- [NO] Renewal date
- [NO] Contact information

Workflow:

1. Redact policy numbers and amounts
2. Assistant updates renewal dates in R-02
3. Assistant flags approaching renewals (90 days out)
4. Principal handles actual renewal (assistant doesn't see amounts)

Task: Organize Physical Documents for Scanning

Documents affected: Various (civil dossier, property deeds, etc.) Protocol:

- Assistant organizes documents by type (passports, deeds, contracts)
- Assistant scans documents
- Assistant uploads to designated folder
- Assistant does NOT open/read documents
- Assistant works in supervised environment (or trusted)

Verification:

- Principal spot-checks folder organization
- Principal verifies document accessibility
- Principal purges any incorrectly filed items

Alternative (high-security):

- Documents placed in sealed envelopes
- Envelopes labeled by type (e.g., "Passports", "Deeds")
- Assistant scans sealed envelopes (envelope becomes scan)
- Principal opens envelopes digitally post-scan

BUREAU SERVICE MODEL

(SIGNUM) Definition: SIGNUM is Standard Index Group's bureau service - administrative tasks performed with redaction-first protocols. Service Tiers:

Tier 1: Document Formatting Only

- Convert handwritten notes to typed P-Series format
- Redact ALL specific details (client provides sanitized input)
- Return formatted template
- Client fills in sensitive data

Example:

```
CLIENT PROVIDES (SANITIZED):
"Bank account at [BANK], expires [DATE], contact [PHONE]"
SIGNUM RETURNS (FORMATTED):
+----------------------------------------+
| Account: [BANK NAME] |
| Number: [ACCOUNT NUMBER] |
| Expiry: [RENEWAL DATE] |
| Contact: [PHONE] |
| Access: [DP REFERENCE] |
+----------------------------------------+
CLIENT FILLS IN BRACKETS WITH ACTUAL DATA
```

Tier 2: Redacted Document Updates

- Client provides redacted copy of existing P-Series instrument
- SIGNUM updates non-sensitive fields per client instruction
- Returns updated redacted document
- Client merges changes into unredacted master

Workflow:

1. Client creates redacted copy (account numbers, balances removed)
2. Client annotates changes needed ("Update address to...")
3. SIGNUM applies changes to redacted copy
4. Client reviews, approves
5. Client manually applies same changes to unredacted master

Tier 3: Supervised Bureau Services

- Client present (physically or virtually) during document handling
- SIGNUM clerk performs tasks under client observation
- Client controls what clerk sees (redacts in real-time or pre-redacts)
- Screen sharing with selective window control

Use case: Complex reorganization tasks requiring judgment but maintaining oversight.

GDPR COMPLIANCE

FRAMEWORK

Data Minimization (Article 5(1)(c)):

Redaction-First Protocol implements data minimization by default:

- Assistants receive only data necessary for task
- No "just in case" data sharing
- Regular audit of what data was shared for what purpose

Purpose Limitation (Article 5(1)(b)):

Defined purposes for data sharing with assistants:

- Document formatting
- Renewal tracking
- Address updates
- Document organization

NOT permitted:

- General "help manage estate"
- Open-ended "organize finances"
- Undefined future purposes

Documentation:

- Each task: documented purpose
- Data shared: logged
- Retention: data deleted after task completion

Storage Limitation (Article 5(1)(e)):

Retention Policy:

- Redacted documents provided to assistant: Retained only during task
- Upon task completion: Assistant deletes all copies
- Verification: Principal requests confirmation of deletion
- Maximum retention: 30 days post-task

Right of Access (Article 15):

If assistant requests data about their access:

- Principal must provide: List of tasks assigned, data shared per task, dates
- Format: Simple log (task, data type, date, deletion date)

OPERATIONAL SECURITY

MEASURES

Communication Channels:

Approved:

- Encrypted email (ProtonMail, Tutanota)
- End-to-end encrypted messaging (Signal)
- Secure file transfer (Tresorit, SpiderOak)

NOT Approved:

- [NO] Standard email (Gmail, Outlook) for sensitive docs
- [NO] SMS/iMessage for document transfer
- [NO] Cloud storage without client-side encryption

Access Control:

Temporary Access:

- Assistant granted access to specific folder for task duration
- Access automatically revoked after task completion
- No persistent access to client files

Audit Trail:

- Log all document access (who, when, what)
- Review logs quarterly
- Investigate anomalous access patterns

Physical Security (Bureau Environment):

If assistant works in bureau office:

- Privacy screens on monitors (prevents shoulder surfing)
- Document shredding immediately after task
- No personal devices in work area
- Supervised or isolated work environment

REDACTION AUDIT CHECKLIST

Before providing document to assistant:

- [ ] Identify task-specific information needed
- [ ] Redact all account numbers
- [ ] Redact all balances/amounts
- [ ] Redact all passwords/credentials (should already be in DP)
- [ ] Redact all personal identifiers (NI numbers, passport numbers)
- [ ] Preserve DP references (ensure visible)
- [ ] Preserve account/institution names (if needed for task)
- [ ] Test redaction (physical: backlight; digital: text select)
- [ ] Document what was shared (log: task, data shared, date)
- [ ] Set retention reminder (delete after task + 30 days)

After task completion:

- [ ] Verify task completed correctly
- [ ] Request assistant confirm deletion of documents
- [ ] Update audit log with completion date
- [ ] Archive redacted version (optional, for audit trail)
- [ ] Review: Was redaction adequate? Document lessons learned

---

CASE STUDY - REDACTION FAILURE

VIII. CASE STUDY: REDACTION FAILURE Incident (2022): Client hired virtual assistant to update P-02 (Accounts Register) with new contact details for various financial institutions. Mistake:

- Client provided unredacted P-02
- Included full account numbers, balances (£12M total across accounts)
- Assistant was untrusted (gig economy worker, minimal vetting)

Consequence:

- Assistant screenshotted document
- Attempted extortion (demanded £50k to not publish)
- Client reported to police
- Criminal prosecution successful (assistant jailed)
- But: Accounts had to be closed and reopened (massive disruption)

Cost:

- 6 months to close/reopen all accounts
- Legal fees: £25k
- Operational disruption: Incalculable
- Emotional distress: Significant

Prevention:

- Redact balances and account numbers (task only needed institution names and contact info)
- Vet assistant properly (or use trusted bureau service)
- Total cost of proper redaction: 15 minutes
- Total cost of failure: £25k + 6 months disruption

Lesson: Redaction is not paranoia. It's basic operational security.

IMPLEMENTATION GUIDE

Step 1: Task Analysis

For each potential assistant task:

1. Define precise task outcome needed
2. List minimum information required
3. Identify all sensitive information in document
4. Design redaction pattern

Example Task Analysis: Task: Update P-09 (Property Folio) with new utility provider contact Needs:

- Property address
- Current utility provider name
- New provider name and contact

Does NOT need:

- Property value
- Mortgage details
- Rental income
- Access codes

Redaction plan:

- Redact valuations
- Redact mortgage information
- Redact rental income figures
- Redact access codes (should already be in DP-xx)
- Preserve addresses, provider names, contact info

Step 2: Create Redaction Template

Create standard redaction patterns for common tasks: Template A: "Address Update Only"

- Redact: Numbers, amounts, codes
- Preserve: Names, addresses, dates

Template B: "Renewal Tracking"

- Redact: Account numbers, amounts
- Preserve: Institution names, expiry dates, contact info

Template C: "Document Organization"

- Redact: All specific content (or seal in envelopes)
- Preserve: Document type label only

Step 3: Document and Log

Maintain Redaction Log:

Date	Task	Document	Data Shared	Assistant	Deletion Date
2024-08-15	Update address	P-02	Account names, addresses	J. Smith	2024-09-15
2024-09-01	Renewal tracking	P-06, R-02	Policy types, expiry dates	J. Smith	2024-10-01

Purpose:

- Audit trail (GDPR compliance)
- Pattern analysis (are we sharing more than needed?)
- Incident investigation (if breach occurs)

CONCLUSION

Administrative delegation is operationally necessary for complex estates. But delegation does not require full information access. The Redaction-First Protocol establishes:

1. Default to redaction - Share only task-necessary information
2. Systematic approach - Checklists and templates prevent oversight
3. GDPR compliance - Data minimization by design
4. Operational security - Limits damage from assistant compromise
5. Audit trail - Document what was shared, when, why

Cost of implementation: 15-30 minutes per task (redaction time) Cost of failure: £10k-£100k+ (breach remediation, legal fees, operational disruption) The choice is clear. Privacy is not achieved by avoiding delegation. Privacy is achieved by disciplined redaction. Expose only what is operationally necessary. Redact everything else.

REFERENCES:

[1] GDPR (EU) 2016/679 - General Data Protection Regulation

Article 5: Principles relating to processing of personal data Article 15: Right of access by the data subject

[2] ICO (UK Information Commissioner's Office) - Data Protection Principles

https://ico.org.uk/for-organisations/guide-to-data-protection/

FOOTER:

PP-01: Redaction-First Protocol v1.2 | Page X of 12 | Standard Index Group | Privacy Protocol

---